Support weight distribution of linear codes

Torleiv Kløve
Department of Informatics, University of Bergen, Bergen, Norway

Received 4 November 1991
Revised 28 January 1992

Abstract

The main result of the paper is expressions for the support weight distributions of a linear code in terms of the support weight distributions of the dual code.

1. Introduction

Let C be an \((n, k)\) code over \(\text{GF}(q)\). For any subcode \(D\) of \(C\), we define the support weight of \(D\) to be the number of positions where not all the codewords of \(D\) are zero, and we denote it by \(w_s(D)\). For \(r \geq 0\) and \(0 \leq i \leq n\), let \(A_i^{(r)}\) be the number of \(r\)-dimensional subcodes of \(C\) of support weight \(i\). The \(r\)th support weight distribution is the sequence
\[
A_0^{(r)}, A_1^{(r)}, \ldots, A_n^{(r)}
\]
and the \(r\)th support weight distribution function is the polynomial
\[
A^{(r)}(Z) = A_0^{(r)} + A_1^{(r)}Z + \cdots + A_n^{(r)}Z^n.
\]
For \(0 \leq r \leq k\), the \(r\)th minimum support weight is defined by
\[
d_r(C) = \min\{w_s(D) \mid D\text{ is an } (n, r)\text{ subcode of } C\} = \min\{i \mid A_i^{(r)} \neq 0\}.
\]
We note that \(A^{(0)}(Z) = 1\). In \([3, 6]\) we studied properties of codes which, by Lemma 1–4 below, are equivalent to support weight distributions; \(A_{ij}\) in \([3, 6]\) is the same as \(A_i^{(j)}\) in the notation above. Among other results in \([3]\), we proved that \(d_r(C) < d_{r+1}(C)\) for all \(r\), a result rediscovered by Wei \([8]\); we also determined the support weight distribution of MDS codes. An application of the

Correspondence to: T. Kløve, Department of Informatics, University of Bergen, Thormøhlensgate 55, 5008 Bergen, Norway.

0012-365X/92/$05.00 © 1992 — Elsevier Science Publishers B.V. All rights reserved
results in [6] was to determine the support weight distribution of the binary
(23, 11) Golay code (without any computer search). Helleseth [2] determined the
support weight distribution of some other classes of codes.

Wei [8] studied the minimum support weights (which he called generalized
Hamming weights) in his analysis of the wire-tap channel of type II. His paper
has sparked renewed interest in the subject. Further recent papers on the
generalized Hamming weights (or minimum support weights) of binary codes are
[1, 4]. Kasami et al. [5] used Wei’s results in their analysis of the state complexity
of the trellis diagrams of some binary codes.

We note that if \( \bar{x} \in GF(q)^n \), then
\[
\text{wt}_H(\bar{x}) = \text{wt}_S(\{ \bar{x} \}) = \text{wt}_S(\{ \lambda \bar{x} \mid \lambda \in GF(q) \}).
\]
Hence,
\[
A^{(0)}(Z) + (q - 1)A^{(1)}(Z) = A(Z),
\]
the Hamming weight distribution function of \( C \), and
\[
d_1(C) = d_{\text{min}}(C).
\]

Let \( B^{(r)}(Z) \) be the \( r \)th support weight distribution function of the dual code \( C^\perp \). We have
\[
B^{(0)}(Z) = 1 = A^{(0)}(Z),
\]
and, by MacWilliams’ identity,
\[
1 + (q - 1)B^{(1)}(Z)
\]
\[
= q^{-k}(1 + (q - 1)Z)^n \left[ 1 + (q - 1)A^{(1)} \left( \frac{1 - Z}{1 + (q - 1)Z} \right) \right].
\]
It is natural to ask if there are similar relations between the polynomials \( B^{(r)}(Z) \)
and \( A^{(r)}(Z) \) for \( r > 1 \). The goal of this paper is to give such relations. Related
results were given in [6].

2. Relations between the support weight distributions of a code and its dual

Let \( G \) be a generator matrix for \( C \), and for any \( \bar{x} \in GF(q)^k \), let \( \mu(\bar{x}) \), the
\textit{multiplicity} of \( \bar{x} \), be the number of occurrences of \( \bar{x} \) as a column in \( G \). Then
\( \text{wt}_S(C) = n - \mu(\bar{0}) \). Let
\[
\mu(U) = \sum_{\bar{x} \in U} \mu(\bar{x}) \quad \text{for any } U \subseteq GF(q)^k.
\]
First we will give an alternative expression for \( \text{wt}_S(D) \), a similar result was given
in [4].

If \( M \) is an \( r \times k \) matrix of rank \( r \), then \( MG \) generates an \( (n, r) \) subcode \( D \) of \( C \),
and any \( (n, r) \) subcode is obtained in this way. Let \( U_D \) be the space orthogonal to
the column space of $M$. Then
\[ w_S(D) = n - \sum_{x \in \mathcal{U}_D} \mu(\tilde{x}) = n - \sum_{x \in \mathcal{U}_D} \mu(\tilde{x}) = n - \mu(U_D). \]

This proves the following lemma.

**Lemma 1.** Let $D$ be a subcode of $C$. Then $w_S(D) = n - \mu(U_D)$.

Let $F_r = \{U \mid U$ is a subspace of $\text{GF}(q)^k$ of dimension $r\}$.

**Lemma 2.** For any $r$ where $0 \leq r \leq k$, $D \mapsto U_D$ is a bijection between the set of $r$-dimensional subspaces of $C$ and the set $F_{k-r}$.

In the sequel, we will use the following further notations:
\[ [a]_b = \prod_{i=0}^{b-1} (q^a - q^i), \]
\[ \langle a \rangle = [a]_n = \prod_{i=0}^{n-1} (q^a - q^i), \]
\[ \binom{a}{b} = \frac{\langle a \rangle}{\langle b \rangle} \] (Gaussian binomial coefficient).

The number of $b$-dimensional subspaces of an $a$-dimensional vector space over $\text{GF}(q)$ is given by the Gaussian binomial coefficient. Also, we note that
\[ [a]_b = \frac{\langle a \rangle}{q^{b(a-b)} \langle a-b \rangle}. \]

Let $C^{(m)}$ be the code generated by $G$ over $\text{GF}(q^m)$.

In [7] we proved the following lemma (in a different notation). An equivalent result was given in [3]. For completeness we include the short proof.

**Lemma 3.** The Hamming weight distribution function for $C^{(m)}$ is
\[ A_m(Z) = \sum_{r=0}^{k} [m]_r \sum_{U \in F_{k-r}} Z^{n-\mu(U)}. \]

**Proof.** Let
\[ \hat{U} = \{ \tilde{y} \in \text{GF}(q^m)^k \mid \tilde{y} \cdot \tilde{x} = 0 \text{ for } \tilde{x} \in \text{GF}(q)^k \text{ if and only if } \tilde{x} \in U \}. \]

We note that if $\tilde{y} \in \hat{U}$, then
\[ w(\tilde{y}G) = \sum_{\tilde{x} \in \text{GF}(q)^k} \mu(\tilde{x})w(\tilde{y} \cdot \tilde{x}) = \sum_{\tilde{x} \in \text{GF}(q)^k \setminus U} \mu(\tilde{x}) = n - \mu(U). \]
We further note that if \( U \in F_r \), then
\[
\sum_{y \in \hat{U}} 1 = [m]_{k-r}.
\]
Since \( \{ \hat{U} \mid U \text{ is a subspace of } GF(q) \} \) is a partition of \( GF(q^m) \), we get
\[
A_m(Z) = \sum_{r=0}^{k} \left( \sum_{\hat{U} \in F_r} Z^{w_{\hat{U}}} \right) = \sum_{r=0}^{k} \sum_{U \in F_r} \sum_{y \in \hat{U}} Z^{n-\mu(U)} = \sum_{r=0}^{k} [m]_{r} \sum_{U \in F_{k-r}} Z^{n-\mu(U)}. \quad \Box
\]

**Lemma 4.** The Hamming weight distribution function \( A_m(Z) \) of \( C^{(m)} \) is
\[
A_m(Z) = \sum_{r=0}^{m} [m]_r A^{(r)}(Z).
\]

**Proof.** Combining Lemmata 1–3 we get
\[
A_m(Z) = \sum_{r=0}^{k} [m]_r A^{(r)}(Z).
\]
Since \([m]_r = 0\) for \( r > m \) and \( A^{(r)}(Z) = 0 \) for \( r > k \), the lemma follows. \( \Box \)

Since \( (C^{(m)})^\perp \) is generated by the parity check matrix of \( C \), the Hamming weight distribution of this code is
\[
B_m(Z) = \sum_{r=0}^{m} [m]_r B^{(r)}(Z).
\]

Hence, MacWilliams' identity for \( C^{(m)} \) gives the following theorem.

**Theorem 1.** For all \( m \geq 0 \) we have
\[
\sum_{r=0}^{m} [m]_r B^{(r)}(Z) = q^{-mk}(1 + (q^m - 1)Z)^{n} \sum_{r=0}^{m} [m]_r A^{(r)} \left( \frac{1 - Z}{1 + (q^m - 1)Z} \right).
\]

From Theorem 1 we can also get an explicit expression for \( B^{(r)}(Z) \) in terms of the \( A^{(r)} \)’s.

**Theorem 2.** For all \( r \geq 0 \) we have
\[
B^{(r)}(Z) = \sum_{j=0}^{r} \sum_{l=0}^{j} (-1)^{j-r} q^{\binom{(j-r)(j-r-1)/2 - (j-r)(j-l-1)}{(j)}(j-l)} \times \{1 + (q^l - 1)Z\}^n A^{(l)} \left( \frac{1 - Z}{1 + (q^l - 1)Z} \right).
\]
Proof. For convenience, we let

$$\alpha_i = q^{-i} \{(q^i - 1)Z\}^n A^{(i)} \left( \frac{1 - Z}{1 + (q^i - 1)Z} \right).$$

Define $\beta_r$ by

$$\beta_r = \sum_{j=0}^r \sum_{l=0}^j (-1)^{j-l} q^{\frac{(r-j)(r-j-1)}{2}} \frac{(r-j)(r-j-l)(j-l)}{(r-j)(j-l)} \alpha_m.$$

Then we have

$$\sum_{r=0}^m [m] \beta_r = \sum_{r=0}^m \sum_{j=0}^r \frac{\langle m \rangle}{q^{(m-1)/2} \langle m-r \rangle} \sum_{l=0}^j (-1)^{j-l} q^{\frac{(r-j)(r-j-1)}{2}} \frac{(r-j)(r-j-l)(j-l)}{(r-j)(j-l)} \alpha_m$$

$$= \sum_{j=0}^m \sum_{l=0}^j \alpha_m q^{j(m-j)-l(j-l)} \frac{\langle m \rangle}{\langle m-j \rangle \langle j-l \rangle}$$

$$\times \sum_{r=j}^m (-1)^{r-j} q^{\frac{(r-j)(r-j-1)}{2}} \frac{(m-r)(r-j)}{(m-j)(r-j)}$$

$$= \sum_{j=0}^m \sum_{l=0}^j \alpha_m q^{j(m-j)-l(j-l)} \frac{\langle m \rangle}{\langle m-j \rangle \langle j-l \rangle}$$

$$\times \sum_{r=0}^m (-1)^{r} q^{\frac{r(r-1)}{2}} \left[ \begin{array}{c} m-j \\ r \end{array} \right]$$

$$= \sum_{l=0}^m \alpha_m q^{-l(m-l)} \frac{\langle m \rangle}{\langle m-l \rangle} = \sum_{l=0}^m \alpha_m [m]_l.$$

since (see e.g. [6, Lemma A.1])

$$\sum_{u=0}^u (-1)^u q^{\frac{u(u-1)}{2}} \left[ \begin{array}{c} u \\ t \end{array} \right] = \begin{cases} 1 & \text{if } u = 0, \\ 0 & \text{if } u > 0. \end{cases}$$

We can now show by induction that $B^{(r)}(Z) = \beta_r$. First,

$$B^{(0)}(Z) = 1 = \beta_0.$$

Next, let $m > 0$ and suppose that $B^{(r)}(Z) = \beta_r$ for $r < m$. Then, by the result just proved above, Theorem 1, and the induction hypothesis,

$$\langle m \rangle B^{(m)}(Z) = \sum_{l=0}^m [m] \alpha_m - \sum_{r=0}^{m-1} [m] B^{(r)}(Z)$$

$$= \sum_{l=0}^m [m] \alpha_m - \sum_{r=0}^{m-1} [m] \beta_r = \langle m \rangle \beta_m. \quad \square$$
As a simple application of Theorem 2, we determine the support weight distributions of the Hamming codes. Let

\[ n = \frac{(q^k - 1)}{(q - 1)}, \]

and let \( G \) be a \( k \times n \) matrix over \( \text{GF}(q) \) containing no zero columns, and no two columns where one is a multiple of the other; that is, \( G \) contains as columns exactly one multiple of each nonzero vector in \( \text{GF}(q)^k \). Let \( C \) be the \((n, k)\) code generated by \( G \). Then \( C^\perp \) is an \((n, n-k)\) Hamming code. If \( D \) is a subcode of \( C \) of dimension \( r \), then, by Lemma 1,

\[ w_s(D) = \frac{q^k - 1}{q - 1} - \frac{q^{k-r} - 1}{q - 1} = \frac{q^k - q^{k-r}}{q - 1}. \]

Hence

\[ A^{(r)}(Z) = \binom{k}{r} Z^{(q^k-q^{r-k})/(q-1)}. \]

By Theorem 2 we get

\[ B^{(r)}(Z) = \sum_{j=0}^{r} \sum_{l=0}^{j} (-1)^{r-j} q^{l(r-j)(r-j-1)/2-l(r-j)-(l-1)-jk} \binom{k}{l} \times \left(1 - Z \right)^{(q^k-q^k^{(r-j)})/(q-1)} \left(1 + (q^l - 1) Z \right)^{(q^l-1)/(q-1)}. \]

References